

## Claims Amended

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Formal Amendment Dated April, 02, 2001	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
Amendment Proposal Dated 7, May 2001			X													X	X	X	X	X	
Amendment Proposal Dated 17, June 2001	X						X			X		X		X		X				X	
Amendment Proposal Dated 22, June 2001	X		X			X	X			X		X		X		X		X	X	X	
Submission of Clean Claims dated 25 June 2001	Amend claims 7, 19 to clear minor typographical errors																				
Submission of New Claim 21 & Amendment on Description	Submit new claim 21, amend minor error in claim 19, amend description and the title being last time amended to be read as "Computer Apparatus/Software Access Right Management"																				
Amendment on Claim 18 Dated Oct., 17, 2001																			X		
Amendment on New Claim 21 Dated Oct., 19, 2001																					X
Last Amendment Dated Oct., 20, 2001																					X
Informal Communication to Examiner Barron Date: Nov., 5, 2001																		X		X	X
Amendment dated 25 Jan., 2002	X									X		X		X				X		X	

*Independent claims = 1, 7, 10, 12, 14, 16, 18, 20, 21*

Marked up  
copy~~-13(Ding)~~

1. (Fifth Time Amended) A method for protecting software from unauthorised use, comprising the steps of:

determining if identity means/information, is existing in a processing apparatus ;

using a favourable result of said determination as a pre-condition for said processing apparatus providing user access to said software desired to be protected ;

wherein said identity means/information being capable of being used [by a control means of said processing apparatus] in enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity means/information being specific to said rightful user(s) and said software desired to be protected being licensed to said rightful user(s).

2. A method for protecting software from unauthorised use , as claimed in claim 1, wherein further comprising the steps of :

authenticating said identity means/information ;

said identity means/information will be determined as existing, if the result of said authentication is favourable and as not existing if otherwise .

3. A method for protecting software from unauthorised use , as claimed in claim 12, wherein said software desired to be protected being first software used on said processing apparatus for determining third information related to hardware and/or software of said processing apparatus ;

wherein further comprising second software for, when being executed, authenticating the computer on which said second software runs as being said processing apparatus, basing on at least a part of said third information;

and access to third software will be provided if said authentication result is favourable .

Marked up copy

-16(Dirty)-

10. (Fifth Time Amended) Authorising program/means used in a processing apparatus, to protect other software against unauthorised use ;

said authorising program/means being for providing access to said software desired to be protected ;

wherein information specific to rightful user(s) of said software desired to be protected, exists in said authorising program/means and being accessible to the user thereof ;

said existing information being capable of being used [, but not in a form as for being so used , by said processing apparatus] in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsible, but not being usable directly by said processing apparatus for said electronic commerce purpose .

11. Authorising program/means as claimed in claim 10, wherein said operation being operation related to making payment from an account of said rightful user(s).

12. (Fourth time Amended)A method for protecting software from unauthorised use , comprising the steps of :

obtaining a first information from a user of a processing apparatus having an identity software/means ;

using said first information received being correct as a pre-condition for said processing apparatus providing user access to said software desired to be protected;

wherein said identity software/means being for providing a second information specific to rightful user(s) of said software desired to be protected, if said correct first information is being obtained from a user thereof ; and said second information being capable of being used [by said proccssing apparatus] in enabling electronic commcrce operation(s) for which said rightful user(s) has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed.

marked  
up  
copy

-17(Dirty)-

13. A method for protecting software from unauthorised use, as claimed in claim 12, wherein said operation being operation related to making payment from an account of said rightful user(s) and said first information being a password.

14. (Fourth Time Amended) A method for protecting software from unauthorised use , comprising the steps of :

authenticating identity information/means associated with [a control means of] a processing apparatus;

using a favourable result of said authentication as a pre-condition for said processing apparatus providing user access to said software desired to be protected ;

wherein said identity information/means being capable of being used [by said control means] in enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity information/means being specific to said rightful user(s) and said software desired to be protected being licensed to said rightful user(s) .

15. A method for protecting software from unauthorised use , as claimed in claim 14, wherein said operation being operation related to making payment from an account of said rightful user(s).

marked up  
copy

-19(Dirty)-

18. (Fifth time Amended) A method for protecting software from unauthorised use, by restricting the use thereof to a single person, comprising the steps of :

- a) supplying said software desired to be protected, first software and second software to a processing apparatus, say, first processing apparatus ;
- b) running said first software on said processing apparatus ;
- c) establishing a communication between said first software running on said processing apparatus, and a remote electronic transaction system ;
- d) verifying said person having a valid account, by said remote electronic transaction system ;
- e) using by said first software, a favourable result of said verification as a pre-condition for determining from said processing apparatus information related to the hardware or/and software thereof, for future reference in step f) below ;

wherein a cost is being charged from said account for the first time said steps a) to c) being carried out ; thereafter

- f) authenticating by said second software, the processing apparatus on which said second software is being used, say, second processing apparatus, basing on at least a part of said information related to said hardware or/and software ;
- g) using by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus, with no charge ;

if the result of said authentication is not favourable, repeat at least said steps c) to e) with said second processing apparatus, without re-charging from said account said cost .

marked  
copy

-21(Dirty)-

20. (Fifth time Amended) A method for protecting software, publicly distributed through a communications network, for use by a user, from unauthorised use, comprising the steps of :

a) creating first software ;

wherein "the presence of identity information/means [which being specific to said user of said software desired to be protected and being used in enabling operation(s) for which said user has to be responsible,] in a processing apparatus" is being used in the creation of said first software as a pre-condition for said first software to perform step c) below ; and said identity information/means being specific to said user of said software desired to be protected and capable of being used in enabling electronic commerce operation(s) for which said user has to be responsible ;

b) running said first software on said processing apparatus ;

c) determining by said first software running on said processing apparatus meeting said precondition, first information related to the hardware or/and software of said processing apparatus, for future reference in step e) below ;

d) thereafter, determining by second software, from the processing apparatus onwhich said second software is being used, second information related to the hardware or/and software thereof;


e) determining by said second software, if said second information is consistent with said first information ;

f) using by said second software, a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on the processing apparatus onwhich said second software is being used ;

repeat at least said step c) with the processing apparatus on which said second software is being used if said result of said determination of consistence is not favourable, without causing any user responsible operation(s) being performed .

Clean w/ly

-13(Clean)-

- 
1. A method for protecting software from unauthorised use, comprising the steps of:  
determining if identity means/information, is existing in a processing apparatus ;  
using a favourable result of said determination as a pre-condition for said processing apparatus providing user access to said software desired to be protected ;  
wherein said identity means/information being capable of being used in enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;  
wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity means/information being specific to said rightful user(s) and said software desired to be protected being licensed to said rightful user(s).
2. A method for protecting software from unauthorised use , as claimed in claim 1, wherein further comprising the steps of :  
authenticating said identity means/information ;  
said identity means/information will be determined as existing, if the result of said authentication is favourable and as not existing if otherwise .
3. A method for protecting software from unauthorised use , as claimed in claim 12, wherein said software desired to be protected being first software used on said processing apparatus for determining third information related to hardware and/or software of said processing apparatus ;  
wherein further comprising second software for, when being executed, authenticating the computer on which said second software runs as being said processing apparatus, basing on at least a part of said third information;  
and access to third software will be provided if said authentication result is favourable .

clean copy

-16(Clean)-

10. Authorising program/means used in a processing apparatus, to protect other software against unauthorised use ;

said authorising program/means being for providing access to said software desired to be protected ;

wherein information specific to rightful user(s) of said software desired to be protected, exists in said authorising program/means and being accessible to the user thereof ;

said existing information being capable of being used in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsible, but not being usable directly by said processing apparatus for said electronic commerce purpose .

11. Authorising program/means as claimed in claim 10, wherein said operation being operation related to making payment from an account of said rightful user(s).

12. A method for protecting software from unauthorised use , comprising the steps of :

obtaining a first information from a user of a processing apparatus having an identity software/means ;

using said first information received being correct as a pre-condition for said processing apparatus providing user access to said software desired to be protected;

wherein said identity software/means being for providing a second information specific to rightful user(s) of said software desired to be protected, if said correct first information is being obtained from a user thereof ; and said second information being capable of being used in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed.



clean copy

-17(Clean)-

13. A method for protecting software from unauthorised use, as claimed in claim 12, wherein said operation being operation related to making payment from an account of said rightful user(s) and said first information being a password.

14. A method for protecting software from unauthorised use, comprising the steps of:  
authenticating identity information/means associated with a processing apparatus;

using a favourable result of said authentication as a pre-condition for said processing apparatus providing user access to said software desired to be protected;

wherein said identity information/means being capable of being used in enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity information/means being specific to said rightful user(s) and said software desired to be protected being licensed to said rightful user(s).

15. A method for protecting software from unauthorised use, as claimed in claim 14, wherein said operation being operation related to making payment from an account of said rightful user(s).

*clear copy*

-19(Clean)-

18. A method for protecting software from unauthorised use, by restricting the use thereof to a single person, comprising the steps of :

- KB*  
*L2*  
*cont*
- a) supplying said software desired to be protected, first software and second software to a processing apparatus, say, first processing apparatus ;
  - b) running said first software on said processing apparatus ;
  - c) establishing a communication between said first software running on said processing apparatus, and a remote electronic transaction system ;
  - d) verifying said person having a valid account, by said remote electronic transaction system ;
  - e) using by said first software, a favourable result of said verification as a pre-condition for determining from said processing apparatus information related to the hardware or/and software thereof, for future reference in step f) below ;

whercin a cost is being charged from said account for the first time said steps a) to e) being carried out ; thereafter

- f) authenticating by said second software, the processing apparatus on which said second software is being used, say, second processing apparatus, basing on at least a part of said information related to said hardware or/and software ;
- g) using by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus, with no charge ;

if the result of said authentication is not favourable, repeat at least said steps c) to e) with said second processing apparatus, without re-charging from said account said cost .

clean up

-21(Clean)-

20. A method for protecting software, publicly distributed through a communications network, for use by a user, from unauthorised use, comprising the steps of :

a) creating first software ;

wherein "the presence of identity information/means in a processing apparatus" is being used in the creation of said first software as a pre-condition for said first software to perform step c) below ; and said identity information/means being specific to said user of said software desired to be protected and capable of being used in enabling electronic commerce operation(s) for which said user has to be responsible ;

b) running said first software on said processing apparatus ;

c) determining by said first software running on said processing apparatus meeting said precondition, first information related to the hardware or/and software of said processing apparatus, for future reference in step e) below ;

d) thereafter, determining by second software, from the processing apparatus on which said second software is being used, second information related to the hardware or/and software thereof;

e) determining by said second software, if said second information is consistent with said first information ;

g) using by said second software, a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on the processing apparatus on which said second software is being used ;

repeat at least said step c) with the processing apparatus on which said second software is being used if said result of said determination of consistence is not favourable, without causing any user responsible operation(s) being performed